DEFENSE INTELLIGENCE AGENCY

Department of Defense
Intelligence Management System

SECURITY ANALYSIS

Prepared for:
DoDIMS PMO
National Intelligence Production Center
DIA/PO-5C

Prepared by:
J.G. Van Dyke & Associates, Inc.
6550 Rock Spring Drive, Suite 360
Bethesda, Maryland 20817

November 30, 1994

Table of Contents

Section **Page**

1.0 Executive Summary 1

2.0 Background 2

3.0 Purpose 2

4.0 Safeguards and Analysis 2

4.1 Conceptual Design 2
4.2 Mode of Operation 2
4.3 Identification of All Accrediting Authorities 3
4.4 System Security Plan 3
4.5 Appointment of ISSO 3
4.6 Access by Foreign Nationals 3
4.7 Accreditation 3
4.8 Joint Accreditations 3
4.9 Interim Approval to Operate 3
4.10 Security Briefings 3
4.11 Automated Guard Processors 3
4.12 Protection of High Density/Transportable Storage Devices 3
4.13 Memory Remanence 4
4.14 Protected Software and Hardware 4
4.15 Shipment of Equipment to High-Risk Area 4
4.16 Marking Storage Media 4
4.17 Marking Printed Output 4
4.18 Manual Review of Human Readable Output 4
4.19 System Disposal Plan 4
4.20 COMSEC 4
4.21 Use of Dial-Up Lines 4
4.22 TEMPEST 5
4.23 Physical Security 5
4.24 Personnel Security 5
4.25 Commercial Vendor Maintenance 5
4.26 Technical Requirements for System High Mode 5
4.27 AUTODIN Connectivity 6
4.28 DODIIS Network Connectivity 6
4.29 Connectivity to Other AISs and Networks 6
4.30 Personal Computer Security Requirements 7
4.31 System High Mode Workstation Requirements 7

Section **Page**

5.0 Exceptions to Security Requirements 7

6.0 Vulnerabilities and Levels of Risk 7

APPENDIX A 8

1.0 **Executive Summary**

The Department of Defense (DoD) Intelligence Management System (DoDIMS) is a software application designed to support the DoD and National intelligence communities in registering, validating, tracking and managing production requirements. It provides the mechanism for scheduling, deconflicting, assigning production and most importantly, provides the capability to track and manage overall production activities across operational and national planners and consumers. The DoDIMS program is structured under the definition of a DoD Intelligence Information System (DoDIIS) Core product. DoDIMS will operate in a system high mode at the Top Secret (TS), Sensitive Compartmented Information (SCI) Level.

DoDIMS will function as a client-server application using the Joint Deployable Intelligence Support System (JDISS) to host the DoDIMS application. Through a replication server process, each DoDIMS site will update other DoDIMS peer databases. Thus, a local site will have a read/write capability of its respective data but read only capability of data respective of remote, peer sites. Eventually, a master, read-only DoDIMS database will be established at the Defense Intelligence Analysis Center. The Joint World-wide Intelligence Communications System (JWICS) will provide the network support for DoDIMS client-server communications. Use of JDISS, a current operational and accredited system, will allow connectivity with other intelligence systems required to support users during peacetime, crises, and wartime. The DoDIMS user will, therefore, have an integrated and interoperable tactical intelligence capability that includes host access, electronic mail, message handling, image processing, motion video processing and graphics capability.

DoDIMS employs an open systems architecture through the use of standards consistent with existing DoD, Department of Commerce, DoDIIS, National Institute of Standards and Technology (NIST), and Open Standards Institute(OSI)/Government Open Systems Interconnection Profile (GOSIP) standards. DoDIMS is an application hosted on a JDISS workstation. The workstation will reside in a user activity SCI Facility (SCIF) which must comply with the Communications Security (COMSEC) and physical security requirements for any system processing SCI data. DoDIMS can be loaded with data from UNCLASSIFIED to SCI levels, depending on the information provided by the users. In order to ensure compliance with security regulations regarding the different classification levels of the data, the DoDIMS/JDISS workstation operates at the SCI level. Each workstation is essentially autonomous, except that through the replication server process each replicates a copy of its data (the production requirement transaction) to all other interested DoDIMS/JDISS workstations over the Defense Secure Network 3 (DSNET3), because of the possibility of SCI information in the transaction. A local DoDIMS user may only "read" data that has been replicated by a remote DoDIMS workstation.

This document provides the means for defining the basic sources and types of security requirements for the SCI DoDIMS. The security requirements are necessary to maintain an acceptable level of risk for the intelligence information processed and stored by DoDIMS. The security requirements identified in this document are specifically derived from the functional requirements for DoDIMS and the DoDIMS Security Concept of Operations, as well as from DIA and DoD directives concerning the security of SCI data.

A key issue in the security accreditation of DoDIMS is the fact that DoDIMS will operate under the UNIX operating system, specifically, the Sun Solaris operating system, version 1.1, enhanced by the Sun Basic Security Module version 4.1.3. Many of the security requirements will be implemented by the operating system and by the Sybase Database Management System (DBMS) which holds the DoDIMS data tables.

2.0 **Background**

The functional requirements for DoDIMS are addressed in the DoDIMS Security Concept of Operations (SECONOPS) 16 July 1993. The SECONOPS addresses the basic system design and architecture, discusses how the system is used, and provides a foundation of security requirements outlined in this document. The specific security test procedures used for accreditation of DoDIMS were developed form appropriate security guidelines after being defined by the requirements document.

3.0 **Purpose**

Because the DoDIMS application must operate in the SCI environment for the user to accomplish his mission, there are many security requirements which it must meet in order to be accredited at the SCI level. This DoDIMS Security Analysis document identifies those security requirements and provides a vehicle for recording the minimum technical and non-technical requirements for an automated information system (AIS) like DoDIMS which processes U.S. intelligence information. Additionally, this document provides a vehicle for recommending and analyzing appropriate safeguards to fulfill the security requirements. This document is an amplification of requirements set forth in the DIA Supplement to DIA Regulation (DIAR) 50-11; DIAR 50-23; and DIA Manual (DIAM) 50-5, Vol II (referred to as the "Systems Security Handbook" or simply "the Handbook".

4.0 **Safeguards and Analysis**:

Planned safeguards to fulfill the administrative, environmental, and technical security requirements are described below.

4.1 Conceptual Design

DoDIMS has been developed using a systems engineering approach.

4.2 Mode of Operation

DoDIMS operates in the system high mode of operation at the TS/SI/TK level, as defined in DDS-2600-5502-87 and Section 4 of the DoDIMS Security Concept of Operation.

4.3 Identification of All Accrediting Authorities

DIA/SY-1D is the Designated Accrediting Authority for DoDIMS.

4.4 System Security Plan

See the DoDIMS System Security Plan, dated 14 November 1994. *Each DoDIMS site will supplement this Plan as necessary.*

4.5 Appointment of ISSO

Each DoDIMS site will appoint an ISSO.

4.6 Access by Foreign Nationals

Foreign nationals will not be authorized or permitted to access DoDIMS.

4.7 Accreditation

DoDIMS will be certified as part of the DIA Site Accreditation accomplished at each DoDIMS site.

4.8 Joint Accreditations

There is no need for Joint Accreditation.

4.9 Interim Approval to Operate

DoDIMS satisfies the requirements for an Interim Approval to Operate.

4.10 Security Briefings

All DoDIMS users will receive AIS security training and security awareness training prior to access to the system.

4.11 Automated Guard Processors

DoDIMS does not have any automated guard processors associated with it.

4.12 Protection of High Density/Transportable Storage Devices

High density/transportable storage devices will be protected as specified in DIAM 50-4 and other regulations and directives pertaining to the protection of SCI data and material.

4.13 Memory Remanence

Site procedures for handling, releasing, and disposing of magnetic media will comply with DIAM 50-4.

4.14 Protected Software and Hardware

DoDIMS hardware, software, and firmware are physically protected within each site's SCIF, and configuration management procedures of the DoDIMS PMO, JDISS PMO and site configuration manager are intended to prevent unauthorized access or modification of hardware and/or software.

4.15 Shipment of Equipment to High-Risk Area

DoDIMS equipment will not be shipped to high risk areas.

4.16 Marking Storage Media - Storage media will be marked at the highest level of security under which DoDIMS operates. Any data downloaded must be marked in accordance with standard DIA marking procedures at the system high level until reviewed by an authorized person and re-classified according to the media's actual content.

4.17 Marking Printed Output

Printed output will have a cover sheet marked with the system high classification. All printed output will be marked with the highest classification of the material. However, until the printed material classification has been verified by reliable human review, all output will be treated at the system high classification.

4.18 Manual Review of Human Readable Output

Manual review by a knowledgeable, authorized person is required when DoDIMS data needs to be sanitized or decompartmented for transfer to another organization or for inclusion into different products.

4.19 System Disposal Plan

The ISSO for each DoDIMS site is responsible for maintaining a system disposal plan.

4.20 COMSEC

DoDIMS will utilize JWICS/DSNET3 for secure communications.

4.21 Use of Dial-Up Lines

Dial-up lines will not be used by DoDIMS.

4.22 TEMPEST

Each DoDIMS site is responsible for ensuring that the DoDIMS/JDISS system is properly installed and that the site meets requisite zoning requirements. Sites with TEMPEST equipment requirements must obtain JDISS compatible TEMPEST-approved equipment.

4.23 Physical Security

DoDIMS/JDISS workstations will only be operated and/or stored in approved SCIFs.

4.24 Personnel Security

The only personnel that have access to DoDIMS are cleared for Top Secret and formally indoctrinated for access to the SI and TK compartments. ISSOs will verify the need-to-know of each individual before allowing him access to DoDIMS data.

4.25 Commercial Vendor Maintenance

Any contractors or technicians who will conduct maintenance will either possess a TS SI/TK clearance or will be under the constant observation of a properly cleared individual. The escort will observe the technician to ensure that no type of storage media is removed or that no unauthorized devices are installed. Maintenance personnel will not be allowed access to DoDIMS data.

4.26 Technical Requirements for System High Mode:

4.26.1 Discretionary Access Control

Provided by Sun OS 4.1.3 and Sybase 10.0.1. See also Security Test 25a.

4.26.2 Object Reuse

Provided partially by Sun OS 4.1.3 and supplemented by site procedures. See also Security Test 25b.

4.26.3 Identification and Authentication

Provided by Sun OS 4.1.3 and Sybase 10.0.1. See also Security Test 25c.

4.26.4 Audit

Provided by Sun OS 4.1.3 and Sybase 10.0.1. See Also Security Test 25d.

4.26.5 System Architecture

The Sun OS 4.1.3 provides the TCB system architecture. See also Security Test 25e.

4.26.6 System Integrity

Provided by Sun OS 4.1.3. See also Security Test 25f.

4.26.7 Security Testing

Provided by DoDIMS Security Test documents. See also Security Test 25g.

4.26.8 Test Documentation

Provided by DoDIMS Security Test documents. See also Security Test 25j.

4.26.9 Design Documentation

Provided by Sun Microsystems vendor documentation and Sybase documentation. See also Security Test 1a.

4.26.10 Identification of User Terminals

Provided by SUN OS 4.1.3. See also Security Test 25l.

4.26.11 Configuration Management

Provided by DoDIMS PMO for DoDIMS application software, and by the JDISS PMO and site hosting the JDISS workstation hardware and software. See also Security Test 25m.

4.27 AUTODIN Connectivity

DoDIMS will not be connected to the AUTODIN network.

4.28 DODIIS Network Connectivity

DoDIMS will be connected to DSNET3/JWICS. Connectivity will be through an accredited site LAN.

4.29 Connectivity to Other AISs and Networks.

DoDIMS will not connect to other AISs or networks.

4.30 Personal Computer Security Requirements

No DOS based PCs will access DoDIMS nor will DoDIMS be hosted on a PC.

4.31 System High Mode Workstation Requirements

Workstations used to access DoDIMS are considered System High workstations since access is gained in the JDISS JWICS/DSNET3 operational environment .

5.0 **Exceptions to Security Requirements**

There are no exceptions to the security requirements.

6.0 **Vulnerabilities and Levels of Risk**

DoDIMS is a UNIX-based application hosted on a Sun SPARCStation 2, 10 or 20 workstation running Sun OS 4.1.3 which satisfies the C2 criteria of the Orange Book. DoDIMS data is maintained in the Sybase DBMS which provides additional security protection. DoDIMS, therefore, satisfies the minimum requirements for a system operating in the system high mode of operation. As systems operating at the C2 level are dependent on procedural and environmental security measures, there is some risk that human error or malfeasance could jeopardize the security of the system. Since DoDIMS operates in a SCIF environment with strict personnel and physical security requirements, the level of risk is considered to be low.

APPENDIX A
Terms and Abbreviations

AIS	Automated Information System
AUTODIN	Automatic Digital Network
COMSEC	Communications Security
DAA	Designated Accrediting Authority
DBMS	Database Management System
DCID	Director of Central Intelligence Directive
DIA	Defense Intelligence Agency
DIAM	DIA Manual
DIAR	DIA Regulation
DoD	Department of Defense
DoDIIS	DoD Intelligence Information System
DoDIMS	DoD Intelligence Management System
DSNET3	Defense Secure Network 3
GOSIP	Government Open Systems Interconnection Profile
ISSO	Information System Security Officer
JDISS	Joint Deployable Intelligence Support System
JWICS	Joint World-wide Intelligence Communications System
LAN	Local Area Network
NIST	National Institute of Standards and Technology
OSI	Open Systems Institute
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facility
SECONOPS	Security Concept of Operations
SSRD	System Security Requirements Document
TCB	Trusted Computer Base